ABSTRACT OF THE DISCLOSURE

STORING KEYS IN A TCPA CRYPTOLOGY DEVICE

A method and system for managing cryptology keys in a TCPA subsystem such as a Trusted Platform Module (TPM). The TPM encrypts/decrypts data being communicated with a processing system. Internal to the TPM is limited memory for storing cryptology private keys used in the encryption/decryption. Under the TCPA specification, the keys are hierarchical, such that a parent key must be in the TPM to load into the TPM the requested child cryptology private key. Thus there is an expense associated with replacing an existing key. This expense is determined by the probability that the evicted key will be needed and thus re-stored in the future and the likelihood that ancestor keys will have to be loaded into the TPM in order to load the requested child key. The present invention presents a method for determining this expense, in order to determine which key should be evicted.